Transcript for:

FFIEC Industry Outreach:
Financial Sector Cybersecurity Resources
October 31, 2018

Hello and welcome to the FFIEC Industry Outreach webinar. I'm Jean Roark, and I'll be your facilitator.

Today, we'll discuss Financial Sector Cybersecurity Resources. Let me introduce our speakers.
Mary Aiken is from the Federal Reserve Board of Governors, Ernie Chambers is from the Office of the Comptroller of the Currency, and Rick Lichtenfels is from the Department of Homeland Security.

Before turning the call over to Mary Aiken, I'll run through our call logistics.

If you haven't joined us through the webinar yet, go ahead and click the link you received after registering. For the best webinar experience, use the FAQ document, which can be found using the Materials button in the webinar player page. I'll highlight a few important notes for you:

Upon entering the webinar, you were automatically set up to stream the audio through your computer speakers.

But if you have audio issues, you can dial in through the phone. The connection information is listed in the webinar player page. It's important to note that if you choose to use the phone option, slides will not sync with audio unless you change your settings. You can do this by selecting the gray gear located on the upper right corner of the slide window just above the presentation. From there, you should see a few options in the media chooser, and you should select the phone option if you're listening to the audio through the phone.

You can expand the size of the slides. To do this, use the maximize button in the upper right corner of the slide window located on the webinar player page.

If you'd like a PDF version of today's presentation, you can access it using the Materials button.

We're offering closed captioning for today's webinar. To use this function, select the CC button in the webinar player page.

And, you can send in your questions any time during our call. If you've joined us via webinar, just use the "Ask Question" button.

Okay, let me cover the legal language on slide 2 before turning it over to our presenters. This program is being offered through the Federal Financial Institutions Examination Council, also known as the FFIEC.

Use of these materials by participants, including video and audio recording of this presentation, is strictly prohibited except by written permission of the FFIEC or its members. The views expressed in this presentation are individual views, intended for informational purposes, and are not formal opinions of, nor binding on, the FFIEC or its members.

It is now my pleasure to turn the call over to Mary Aiken from the Federal Reserve.

>> Welcome to a Federal Financial Institutions Examination Council, which is also known as the FFIEC, webinar focused on Cybersecurity month. I'm Mary Aiken, the FFEIC Task Force on Supervision Chair and the Board of Governors' member on that task force.

This October, National Cybersecurity Awareness Month is commemorating its 15th year as an annual initiative to raise awareness about the importance of cybersecurity. In recognition of the need to support this vital mission, the FFIEC is publishing a Cybersecurity Resources Guide for financial institutions.

The programs and initiatives included in the guide are designed for, or otherwise are available to, financial institutions. These resources are actionable and can help financial institutions meet their control objectives regardless of whether they use the FFIEC Cybersecurity Assessment Tool, the NIST Cybersecurity Framework, Financial Services Sector Specific Cybersecurity Profile, or any other methodology to assess their cybersecurity preparedness.

The resources are divided into four types: assessments, exercises, information sharing, and response and reporting. The first page of the guide identifies 16 cybersecurity resources and whether they are free, a paid-for service, or a combination thereof. The subsequent pages provide a detailed overview of the services, as well as information on how to contact each resource.

Use of any of these resources is voluntary, and the FFIEC members do not endorse any of the listed organizations.

Thank you for your participation in today's event, and we hope you will find this webinar useful. Ernie Chambers will speak with you next regarding cybersecurity resources.

>> The assessment resources provide a method by which an institution can evaluate its cybersecurity practices. There are a number of freely available resources from the Department of Homeland Security, or DHS, and the Center for Internet Security, also known as CIS, including:

DHS's National Cybersecurity and Technical Services offerings,

DHS's Cyber Resilience Review, and

CIS's Benchmarking Resources.

DHS offers two assessment resources listed in the guide. First, the DHS National Cybersecurity

Assessments and Technical Services, or NCATS, team is a part of the National Cybersecurity and Communications Integration Center. It supports U.S. government and industry critical infrastructure by providing proactive testing and assessment services. One of the primary services offered by NCATS is its Cyber Hygiene program, which aims to secure Internet-accessible systems by continuously scanning for known vulnerabilities and configuration errors. NCATS services are available at no cost to financial institutions.

Additionally, the DHS Cyber Resilience Review, CRR, is a free, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains, including risk management, incident management, and service continuity. The CRR assessment is designed to measure existing organizational resilience, as well as provide a gap analysis for improvement based on recognized best practices.

Finally, CIS is a non-profit entity that provides a number of resources to the global IT community to safeguard private and public organizations against cyber threats. CIS offers free benchmarking and configuration assessment tools for common applications and operating systems that can be leveraged by institutions when securing their systems.
The cyber exercise resources provide the financial institution a means to test its preparedness to respond to a cybersecurity incident. The exercise resources identified in the guide are:
FDIC Cyber Challenge: A Community Bank Cyber Exercise,
Financial Sector Cyber Exercise Template, and
FS-ISAC Cyber Attack Against Payment Systems Exercise, known as CAPS.

The FDIC Cyber Challenge exercises provide nine video vignettes that help community financial institutions facilitate discussions about operational risk issues and the potential impact of IT disruptions on common banking functions. Two new vignettes were added in October of 2018—one a flood scenario that impacts telecommunications, and the other addressing supply chain risk. The cyber challenges can provide information about an institution's preparedness and identify opportunities to strengthen the bank's resilience to operational risk.

The Financial Sector Cyber Exercise Template is designed for smaller financial sector institutions to test their preparedness. The template helps institutions run their own internal cyber exercises and facilitates discussions on how best to engage with the national architecture for coordinating responses to significant cybersecurity incidents among government and industry. Institutions can modify the template to suit their specific needs.

The FS-ISAC Cyber Attack Against Payment Systems exercise is a two-day, tabletop exercise held annually that simulates an attack on payment systems and processes. The exercise is free and open to non-FS-ISAC members.

Information Sharing Resources [Speaker: Ernie Chambers]
Participating in information-sharing forums is an important element of a financial institution's risk

management processes and its ability to identify, mitigate, and respond to cybersecurity threats and incidents. There are a number of information-sharing resources available through government and industry. Some of the key information-sharing resources identified in the guide are:
DHS Automated Information Sharing Program,
FS-ISAC,
InfraGard,
National Credit Union Information Sharing and Analysis Organization, or NCU-ISAO,
U.S. Secret Service Electronic Crimes Task Force,
Financial Crimes Task Force, and
DHS National Cybersecurity and Communications Integration Center, or the NCCIC.

The Automated Information Sharing Program, or AIS, is a part of the DHS's effort to create an ecosystem in which indicators of an attempted compromise at a company or federal agency can be shared in real time with all partners, protecting them from that particular threat.

The FS-ISAC is a global financial industry resource for sharing cyber and physical threat intelligence and analysis. Membership in the FS-ISAC is tiered and based on institution size. FS-ISAC also offers a free service to provide the most critical public alerts through its Critical Notification Only Participant program.

InfraGard is a partnership between the Federal Bureau of Investigation and members of the private sector. The InfraGard program provides a vehicle for public and private collaboration that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure.

The mission of the National Credit Union Information Sharing and Analysis Organization, or NCU-ISAO, is to enable and sustain Credit Union critical infrastructure cyber resilience and preserve the public trust by advancing trusted security coordination and collaboration to identify, protect, detect, respond, and recover from threats and vulnerabilities.

The Secret Service has established 40 Electronic Crimes Task Forces in the United States. The mission of this network is to prevent, detect, and investigate electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems. The task forces leverage the combined resources of academia; the private sector; and local, state, and federal law enforcement.

The Secret Service also has established 46 Financial Crimes Task Forces in the United States. They combine the resources of the private sector and other law enforcement agencies in an organized effort to combat threats to U.S. financial payment systems and critical infrastructures.

The mission of the DHS National Cybersecurity and Communications Integration Center, or NCCIC, is to reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center. As part of the NCCIC, the United States Computer Emergency Readiness Team, or US-CERT, responds to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners

around the world. US-CERT regularly publishes timely information about current vulnerabilities, exploits, and other security issues.

Cyber incident management involves strong response capabilities, including knowing where to report incidents. The following resources can support an institution's incident response and reporting capabilities, as well as help inform law enforcement of the evolving threats facing the financial sector:
DHS Cyber Incident Reporting Guide,
FBI's Internet Crime Complaint Center, known as IC3,
Financial Crimes Enforcement Network, or FinCEN,
Sheltered Harbor, and
Reporting to Primary Regulators.

DHS's Cyber Incident Reporting Guide provides details regarding the importance of reporting cyber incidents. For instance, private sector entities that are the victim of a cyber incident can receive assistance from government agencies that are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. Federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery in a significant event. The DHS Cyber Incident Reporting Guide details these efforts.

The mission of the Internet Crime Complaint Center, IC3, is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

FinCEN's mission is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. Cybercriminals target the financial system to defraud financial institutions and their customers and to further other illegal activities. Financial institutions can play an important role in protecting the U.S. financial system from these threats. Institutions should determine if filing a Suspicious Activity Report, or SAR, is required or appropriate, as in the case of an unauthorized electronic intrusion intended to damage, disable, or otherwise affect critical systems. When filing is not required, institutions may file a SAR voluntarily to aid law enforcement in protecting the financial sector. Financial institutions are encouraged to provide relevant cyber-related information and indicators in their SAR reporting. Additionally, financial institutions can register with FinCEN to share information, including cyber-related information, with other financial institutions regarding individuals, entities, and organizations relating to suspected money laundering and terrorist financing under section 314(b) of the USA PATRIOT Act.

Sheltered Harbor is a voluntary industry initiative launched in 2015 following a series of cybersecurity simulation exercises between public and private sectors. Its purpose is to promote the stability and

resiliency of the financial sector and to preserve public confidence in the financial system. The Sheltered Harbor standard combines secure data vaulting of critical customer account information with a comprehensive resiliency plan to provide customers timely access to their account information and underlying funds during a prolonged systems outage or destructive cyber attack. As of October 2018, participating financial institutions hold 70% of U.S. deposit accounts and 55% of U.S. retail brokerage client assets.

In the event that a cyber incident results in unauthorized access to or use of sensitive customer information, the institution may have a responsibility to promptly notify it's federal and state regulators in accordance with the Interagency Guidelines Establishing Information Security Standards implementing the Gramm-Leach-Bliley Act and other applicable federal and state laws. In all instances where institutions are victims of cyber attacks, they are encouraged to inform law enforcement authorities and notify their primary regulators.

For more on how to connect with these programs and initiatives, please see the cybersecurity resource guide on FFIEC.gov's Cybersecurity Awareness page.

Now that we've provided an overview of the guide, I would like to introduce our next speaker, Rick Lichtenfels, Branch Chief of the Cyber Hygiene program. He'll discuss the ongoing efforts of the NCCIC at DHS.

>> Good afternoon. Hi, I'm Rick Lichtenfels from DHS's NCATS program. I'm very honored to be here as part of this FFIEC webinar, and I'm very pleased to speak with you about some of the free, cybersecurity services that DHS provides to both the public and private sector.

So I don't overwhelm everyone with acronyms during my presentation, but for those of you who are not familiar with DHS and our cyber services, I want to let you know that "NCCIC," which you'll hear me refer to frequently, stands for the National Cybersecurity and Communications Integration Center. It's really the hub of DHS cybersecurity services and capabilities.

Now hopefully as I go through these next 10–15 minutes, you'll find these services as exciting and valuable as many other organizations have and you'll look to take advantage of them. DHS—and specifically the NCCIC—cybersecurity services and capabilities cover multiple stages of the NIST Framework.

Within the NCCIC, the NCATS program, which stands for National Cybersecurity Assessments and Technical Services (that's my last acronym, I promise); the NCATS program focuses on the proactive aspect of cybersecurity—so, the "left of boom" stages, if you will.

Within that spectrum, we offer a variety of assessments, penetration testing, and vulnerability scanning services—all of them aimed with the goal of improving the nation's and individual organizations' risk exposure or risk posture.

I'm going to spend the next 10–15 minutes telling you about one of these key services, which is our vulnerability scanning service.

First, let me start off with a little background history on the vulnerability scanning service and some of the major things that have helped get to where we currently are with that service.

NCATS created our vulnerability scanning service in 2012, with a focus of helping Federal Agencies better secure their networks from known cyber vulnerabilities. So when I say "known cyber vulnerabilities," I'm referring to vulnerabilities that have been documented and are well understood and known, as opposed to the zero day exploits that you frequently hear about in the news.

As is the case with many Government programs, often times there's a milestone event or a circumstance that can help really get your program or new capability off the ground. And help folks better understand what it actually brings to bear.

So for NCATS, two big milestones from the early years happened in June of 2013 and April of 2014. The first one, in June of 2013, happened when our program was transferred from a division that was exclusively focused on Federal Network Resilience into the NCCIC. Now what that transfer allowed us to do was it removed the constraint that our services were exclusive to federal government networks and it opened up our ability to partner and provide these services, such as what I am talking about now, to private sector organizations.

The second big milestone from April of 2014 involved the heartbleed vulnerability. This was a pretty big vulnerability. It was pervasive across federal government networks, and over a 17-day period, thanks to our scanning service, we were able to observe a 98% vulnerability reduction across Federal Government networks.

So, this event REALLY demonstrated the effectiveness of our scanning service and how it could be used to help agencies deal with critical vulnerabilities, while also tracking progress in mitigating vulnerabilities across the entire Federal Government space.
Now currently, since we started in 2012 to today, we're scanning over 900 public and private sector stakeholders, and we provide each of these stakeholders with a weekly, organization-specific report, so that they can take the appropriate actions to better secure their networks. So what does this service entail? You're probably wondering how the process works?

Using Nmap, which is a freely available and widely used tool, we scan the most common 1000 TCP ports.

During that scanning process, addresses we find with at least one active port are considered active hosts and then we'll fully port scan those.

Addresses where we don't find any active ports are considered dark space and they'll be rescanned after 90 days just to check for a change in status.

So, organizations that sign up for the service and provide us their IP addresses shouldn't fret if due to our initial scans they have certain address space that is not captured, because we will revisit it.

So active hosts that we find after we go through the full port scans, if they have no vulnerabilities, we'll rescan them every 7 days.

If we find any hosts with vulnerabilities, whether they're low, medium, high, or critical vulnerabilities, we have a rescan policy that revisits these. So, the more serious vulnerabilities are revisited more frequently.

So what constitutes a low, medium, high, or critical vulnerability? Well, our scanning ranks the severity of vulnerabilities using version 2 of the Common Vulnerability Scoring System, or CVSS, which is published within NIST's National Vulnerability Database, with one caveat that if a CVSS score is 10, we rank that severity as Critical.
So, Critical is a 10.0 within that scoring system;
Highs are between 7.0 to 10.0;
Mediums are between 4.0 to 6.9; and then
Low vulnerabilities are anything that score the CVSS score of zero to 3.9.

Now the value of this application within our service, is that we are using a standard scoring system that was developed by NIST, and it's widely understood and used with the community. The algorithm at CVSS is based on, employs multiple variables that account for things such as access complexity, access vector, CIA or confidentiality, integrity, availability impact, the exploitability and remediation level. So, it factors in a lot of different variables, so the organization has a pretty thorough understanding that this is a vulnerability that needs to be taken a little bit more serious, maybe a little less serious. So now you're probably wondering how do I sign up for this service and what does it cost?

Well, as I said at the outset, in terms of cost, this service is completely free.
And basically, as soon as you return the requisite paperwork, we typically can get you signed up within 72 hours and begin scanning your organization within a week.
The three-page agreement that you'll need to sign and return, let's you know where we'll be scanning from, and it also states the goals of the scanning effort, which are three things:

1. One, to identify vulnerabilities on your publicly accessible networks and systems. Now again, in the agreement, you will specify what address space or what you consider publically accessible networks that you want us to scan.
2. Second goal is to provide early warning of specific, actionable vulnerabilities. So, as I mentioned, we'll be scanning, we'll be identifying vulnerabilities, and we're not just going to give you a headache without giving you a pill. We do have remediations or recommendations that we put into the report.
3. The third thing is to inform the government's common operational view of cyberspace. Now in case of federal government networks, our scanning activity helps inform policy and helps us better understand where federal government networks maybe have some weakness or have a little bit of cleaning up we need to do. On the private sector side, it just helps us better

understand trends in industry, so as we develop new services such as the service you'll be signing up for, we can appropriately line up our resources to the needs of the community.

Another thing that you'll see in the agreement, is that we clarify that we won't try to connect to any systems and we won't try to penetrate your network. We're not going to do anything invasive. We're also going to require an email address for us to send the reports, and then we'll be asking for you to provide a POC that's authorized to make changes to the agreement. Now, you can opt in or opt out of the agreement at any time. But again, that POC that's authorized to make changes or change the address space that we scan or anything of that sort, that's going to be critical.

And the only difference, last point I would like to make, between the federal and like the private sector SLTT agreements is that fed agreement has some FISMA language, and we mention also the Trusted Internet Connection and Comprehensive National Cybersecurity Initiative.

So now that you have signed up, you're probably wondering what you will receive?
Well as I mentioned earlier, each of our over 900 stakeholders receives a weekly report of the findings we capture via our scanning service. So on a weekly basis, we will deliver to your POC, or distro, a comprehensive report that details the results of our scan of the IP address space that you specified in your agreement.

This report will detail our methodology and findings, and it'll also contain multiple appendices that help you understand the different aspects of our findings. So it's a lot of information. In fact, the sample report that we have on our website is over 70 pages. So, if you have a large organization, we're going to hit you with a lot of information. Which is good. Smaller organizations obviously have, typically have, smaller reports; but, some of the things you can expect to see in your report, we have appendices that will cover vulnerability changes since the last report. So it'll help you navigate "Hey you scanned me last week and I saw this, and now you scanned me this week and you saw this." So it'll cover some of those changes from report to report.

We'll also have another appendix that will have detailed findings and recommended mitigations. So as I mentioned earlier, we try not to just give you a headache. We also try to give you a pill. So the recommended mitigations are something we take a lot of pride in. Then there's another appendix which provides CVS findings. So we have a file and it's within the PDF, you can just click right on the little icon and it'll give you a CVS file that has all the findings.

And we also have some high-level summaries that show how you're trending in terms of each vulnerability category. And we also tell you your top vulnerabilities by occurrence, whether it's bad SSL certificates or buffer overflows, outdated operating systems or versions, things of that sort.

So in closing, this is a great, free service that we hope everyone takes advantage of.
I do want to stress that this is not a pen test—it's a free view of your externally facing assets.
As a friend of mine put it recently, we're not scanning any more than the bad guys are, we're just kind enough to provide a report with recommendations for fixing the issues.
We do stress that our service should complement your existing security program and capabilities, but

we encourage you to take advantage of this free, third-party, objective perspective of the vulnerabilities present on your externally accessible network assets.
As I mentioned earlier, we are currently scanning over 900 public and private sector stakeholders. We're always happy to sign up additional folks so we can continue furthering our goal of improving national resilience and reducing the risk exposure of as many companies as we possibly can.

I thank you once again for the opportunity to present this exciting service to you, and I sincerely hope we are able to assist your organization with better securing your networks. Thank you very much.

* * * * *

* * * * *